



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/867,648	05/31/2001	Nang Kon Kwan	6502.0345	7988

22852 7590 01/05/2005

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
1300 I STREET, NW
WASHINGTON, DC 20005

EXAMINER

PHAM, KHANH B

ART UNIT	PAPER NUMBER
----------	--------------

2167

DATE MAILED: 01/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/867,648

Applicant(s)

KWAN, NANG KON

Examiner

Khanh B. Pham

Art Unit

2167

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 October 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-6,12,13,16-22 and 28-30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-6,12,13,16-22 and 28-30 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.
2. Applicant's submission filed on October 14, 2004 has been entered.
 - Claims 1, 5, 6, 12, 13, 16, 17, 21, 22, 28, and 29 have been amended.
 - Claims 7-11, 14-15, and 23-27 have been canceled.
 - Claim 30 has been added.
 - Claims 1-6, 12-13, 16-22, 28-30 are pending in this Office Action.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims **1-6, 12-13, 16-22, 28-30** are rejected under 35 U.S.C. 103(a) as being unpatentable over Dulin et al. (US 2002/0029200A1), hereinafter "**Dulin**", and in view of Sinn (US 2002/0166049 A1), hereinafter "**Sinn**".

As per claims 1, 17, 29, Dulin discloses a method, a computer readable medium and a system for validating digital certificates (Page 1, [0007]) having a server (Fig. 2, element 108), an Online Certificate Status Protocol responder (Fig. 2, elements 104), a certificate authority (Fig. 2, element 102) associating a certificate database (Fig. 2, element 214) including records associated with digital certificates, comprising:

- “receiving at the OCSP responder an OCSP request associated with a digital certificate generated by the server” at page 5, [0075], [0077];

(Dulin teaches the relying customer 108 (i.e., “the server”) creates an OCSP request associated with a digital certificate and send to the relying participant 104.)

- “creating by the OCSP responder, a database query based on the received OCSP request” at page 5, [0078]- [0079];

(Dulin teaches the relying participant 104 generate a new request and sends it to the certificate issuing participant 102)

- “sending by the OCSP responder the database query to the certificate database associated with the certificate authority to determine whether the digital certificate is valid” at page 6, [0081];

(Dulin teaches the issuing participant 102 check its customer database 214 to make sure that the request was signed by an entity authorized to make the request)

- “receiving at the OCSP responder a database query result indicating whether the digital certificate matches a corresponding certificate entry stored in one of the certificate database records” at page 6, [0085];

(Dulin teaches the step of sending query result from the issuing participant 102 to the replying participant 104)

- “determining, by the OCSP responder, the validity of the digital certificate based on the database query result” at page 6, [0091]; and “notify the server of the determined validity of the digital certificate.” at page 6, [0092].

The different between the invention of claims 1, 17, 29 and Dulin's teaching is that Dulin teach the step of creating and sending a database query but does not explicitly teach that the database query is a “Lightweight Directory Access Protocol database query” (LDAP) as claimed. However, Sinn teaches a similar method for certificate validation, including a database for storing certificates (Fig. 52, element 36, 2082), wherein the database is an LDAP Directory Server and communicates with other server/modules using LDAP over SSL” at page 6, [0119]. Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Dulin and Sinn's teachings to implement the certificate database using the well-known LDAP directory server as suggested by Sinn, in order to take advantage of

the legacy LDAP directory server to store digital certificates instead of building a new database server for storing digital certificates, and therefore reduces the cost and the complexity of the system.

As per claims 2, 18, Dulin and Sinn teach the method, computer readable medium and system of claims 1, 17 as discussed above. Sinn also teaches: "wherein the Lightweight Directory Access Protocol database query includes an instruction to return a selected portion of a database record" at [0128]-[0129].

As per claims 3, 19, Dulin and Sinn teach the method, computer readable medium of claims 1, 17 as discussed above. Sinn further teaches a Certificate Registration module (Fig. 54) for adding new digital certificates to the database comprising:

- "sending an indication of a new digital certificate from the certificate authority to the certificate database upon issuance of the new digital certificate" at page 31, [0372];
- "receiving, by the certificate database, from the certificate authority, an indication of the new digital certificate; and creating a certificate database record reflecting an identity of the new digital certificate" at page 31, [0374]-[0375].

Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to incorporate Sinn's Certificate registration module into Dulin's

system so that the system would allow adding and certificates to the database and checking status of the certificates when new certificates are issued.

As per claims 4, 20, Dulin and Sinn teach the method and computer readable medium of claims 1, 17 as discussed above. Sinn further teaches the Certificate Registration module for revoking digital certificates comprising the steps of:

- “sending an indication of a revoked digital certificate from the certificate authority to the certificate database upon revocation of the revoked digital certificate” at page 32, [0382];
- “receiving by the certificate database, from the certificate authority, the indication of revocation of the revoked digital certificate” at page 32, [0383];
- “removing a certificate database record associated with the revoked digital certificate from the certificate database” at page 32, [0384] .

Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to incorporate Sinn’s certificate revocation steps into Dulin’s system so that the system would allow revocation of digital certificates and updating the database to reflect the revoked status of the certificates. Maintaining a database with certificate revocation status would allow real time status checking for digital certificates and enable secured transaction based on the status of digital certificates.

As per claims 5, 21, Dulin teaches a method and a computer readable medium in a data processing system for validating digital certificates (page 1, [0007]), the data

Art Unit: 2167

processing system having a certificate authority (Fig. 2, element 102) and a directory server having a database (Fig. 2, elements 202, 212, 214), the method performed by the directory server comprising:

- “maintaining a database of valid digital certificates” at page 21, [0262];
- receiving a query based on an online certificate status protocol request indicating a requested digital certificate” at page 5, [0079];
- “searching the database for a database record reflecting an identity of the requested digital certificate” at page 6, [0081];
- “and returning an indication of the database record when the database record reflecting the requested digital certificate is found to indicate validity of the requested digital certificate” at page 25, [0299]-[0302];
- “whereby the indication of the database record includes meta-data reflecting the validity of the requested digital certificate.” at page 17, [0244]-[0245].

The different between the invention of claims 5, 21 and Dulin's teaching is that Dulin teach the step of receiving a query based on an online certificate protocol request, but does not explicitly teach that the query is a “Lightweight Directory Access Protocol query” as claimed. However, Sinn teaches a similar method for certificate validation, including a database for storing certificates (Fig. 52, element 36, 2082), wherein the database is an LDAP Directory Server and communicates with other server/modules using LDAP over SSL” at page 6, [0119]. Thus, it would have been obvious to one of

ordinary skill in the art at the time of the invention was made to combine Dulin and Sinn's teachings to implement the certificate database using the well-known LDAP directory server as suggested by Sinn, in order to take advantage of the legacy LDAP directory server to store digital certificates instead of building a new database server for storing digital certificates, and therefore reduces the cost and the complexity of the system.

As per claims 6, 22, Dulin and Sinn teach the method and the computer readable medium of claims 5, 21 discussed above. Sinn further teaches a Certificate Registration module (Fig. 54) for adding new digital certificates to the database comprising the steps of:

- "sending an indication of a new digital certificate from the certificate authority to the database upon issuance of the new digital certificate by the certificate authority" at [0372];
- "receiving, by the database from the certificate authority, an indication of the new digital certificate upon issuance of the new digital certificate by the certificate authority" at [0374];
- "and storing a database record reflecting an identity of the new digital certificate" at [0375].

Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to incorporate Sinn's Certificate registration module into Dulin's

system so that the system would allow adding and certificates to the database and checking status of the certificates when new certificates are issued.

As per claims 12, 28, Dulin teaches a method and a computer readable medium in a data processing system for validating digital certificates without certification revocation lists (page 15, [0207]), the data processing system having a client (Fig. 2, element 106), a server (Fig. 2, 108), a responder (Fig. 2, 204), a certificate authority (Fig. 2, 102), associating a database storing records of valid digital certificates of the certificate authority (Fig. 2, 212, 214), the method comprising:

- “generating, by the client, a request for a transaction, the request including a digital certificate identifying the client; receiving the client request by the server” at page 5, [0074];
- “creating, by the server, an online certificate status protocol request based on the associated digital certificate identifying the client” at page 5, [0074];
- “sending, by the server, an online certificate status protocol request to the responder;” at page 5, [0075];
- “receiving, by the OCSP responder, the online certificate status protocol request associated with the digital certificate” at page 5, [0077];
- “creating, by the responder, a database query based on the received online certificate status protocol request” at page 5, [0079];

- “sending, by the responder, the database query to the database associated with the certificate authority to determine whether the digital certificate is valid” at page 5, [0079];
- “searching the database for a database record identifying the digital certificate associated with the online certificate status protocol request” at page 6, [0081];
- “returning a database query result indicating whether the database record identifying the digital certificate is stored in the database,” at page 7, [0094];
- “sending, by the responder, a validity indication whether the digital certificate is valid based on the query result to the server” at page 25, [0299]-[0302];
- “sending, by the server to the client, an indication of whether the transaction is authorized based on the validity indication” at page 7, [0095].

The different between the invention of claims 12, 28 and Dulin's teaching is that Dulin teach the step of creating and sending a database query but does not explicitly teach that the database query is a “Lightweight Directory Access Protocol database query” (LDAP) as claimed. However, Sinn teaches a similar method for certificate validation, including a database for storing certificates (Fig. 52, element 36, 2082), wherein the database is an LDAP Directory Server and communicates with other server/modules using LDAP over SSL” at page 6, [0119]. Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to

combine Dulin and Sinn's teachings to implement the certificate database using the well-known LDAP directory server as suggested by Sinn, in order to take advantage of the legacy LDAP directory server to store digital certificates instead building a new database server for storing digital certificates, and therefore reduces the cost and the complexity of the system.

As per claim 13, Dulin teaches a data processing system for answering online certificate status requests without certificate revocation lists (page 15, [0207]), comprising "a memory having program instructions; a processor configured to execute the program instructions" (page 22, [0272]) to:

- "receive from a server an online certificate status protocol request associated with a digital certificate" at page 5, [0074];
- "create a database query based on the received request, send the database query to a database associated with a certificate authority to determine whether the digital certificate is valid" at page 5, [0079],
- "receive a database query result from the database indicating whether the digital certificate matches a corresponding entry stored in a database one of the certificate database record" at page 6, [0081],
- "determine the validity of the digital certificate based on the database query result" at page 7, [0094],

- “and notify the server of the determined validity of the digital certificate” at page 7, [0095].

The different between the invention of claim 13 and Dulin's teaching is that Dulin teach the step of creating and sending a database query but does not explicitly teach that the database query is a “Lightweight Directory Access Protocol database query” (LDAP) as claimed. However, Sinn teaches a similar method for certificate validation, including a database for storing certificates (Fig. 52, element 36, 2082), wherein the database is an LDAP Directory Server and communicates with other server/modules using LDAP over SSL” at page 6, [0119]. Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Dulin and Sinn's teachings to implement the certificate database using the well-known LDAP directory server as suggested by Sinn, in order to take advantage of the legacy LDAP directory server to store digital certificates instead building a new database server for storing digital certificates, and therefore reduces the cost and the complexity of the system.

As per claim 16, Dulin teaches a data processing system for answering online certificate status requests without certificate revocation lists (page 15, [0207]), comprising:

- “a client computer configured to send a request for a transaction, the request including a digital certificate identifying the client” at Fig. 2, element 106 and page 5, [0074];

- “a server computer (Fig. 2, element 108) configured to receive the client request” (page 5, [0074]), create an online certificate status protocol request based on the associated digital certificate identifying the client and send the online certificate status protocol request” at page 5, [0074];
- “an OCSP responder configured to receive the online certificate status protocol request associated with the digital certificate” at page 5, [0077];
- “create a database query based on the received online certificate status protocol request” at page 5, [0079], and send the database query to determine whether the digital certificate is valid” at page 6, [0081];
- “a certificate authority that provide valid digital certificates” at Fig. 2, element 102 and page 1, [0007];
- “ a database associated with the certificate authority storing records of valid certificates of the certificate authority (Fig. 2, element 214) and configured to search for a database record identifying the digital certificate associated with the online certificate status protocol request” at page 5, [0079], [0081];
- “return an database query result indicating whether the digital certificate matches one of the records stored in the database” at page 6, [0085].
- “wherein the OCSP responder determines that the digital certificate is valid when it receives an database query result reflecting that the digital certificate matches one of the database records” at page 6, [0091]-[0092].

The different between the invention of claim 16 and Dulin's teaching is that Dulin teach the step of creating and sending a database query but does not explicitly teach that the database query is a "Lightweight Directory Access Protocol database query" (LDAP) as claimed. However, Sinn teaches a similar method for certificate validation, including a database for storing certificates (Fig. 52, element 36, 2082), wherein the database is an LDAP Directory Server and communicates with other server/modules using LDAP over SSL" at page 6, [0119]. Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Dulin and Sinn's teachings to implement the certificate database using the well-known LDAP directory server as suggested by Sinn, in order to take advantage of the legacy LDAP directory server to store digital certificates instead building a new database server for storing digital certificates, and therefore reduces the cost and the complexity of the system.

As per claim 30, Dulin and Sinn teach the method according to claim 1 discussed above. Dulin also teaches:

- "the server and the OCSP responder reside in a first computer network" at Fig. 2, elements 104, 108;
- "the certificate authority and the certificate database reside in a second computer network" at Fig. 2, element 102, 214;
- "the first computer network is connected to the second computer network via a computer network firewall" at page 16, [0229] and page 25, [0306].

Response to Arguments

5. Applicant's arguments filed October 14, 2004 have been considered but are moot in view of the new ground(s) of rejection.

Applicant argued that Sinn does not teach the steps of: "receiving, at the OCSP responder, an OCSP request associated with a digital certificates generated by the server" nor "sending, by the OCSP responder, the lightweight Directory Access Protocol database query to the certificate database associated with the certificate authority to determine whether the digital certificate is valid". However, as presented in section 4 above, Dulin teaches the step of: "receiving, at the OCSP responder, an OCSP request associated with a digital certificates generated by the server" at page 5, [0074] and [0077]; Dulin also teaches the step of "sending by the OCSP responder, the database query to the certificate database associated with the certificate authority to determine whether the digital certificate is valid" at page 6, [0081].

Dulin teach the step of creating and sending a database query but does not explicitly teach that the database query is a "Lightweight Directory Access Protocol database query" (LDAP) as claimed. However, Sinn teaches a similar method for certificate validation, including a database for storing certificates (Fig. 52, element 36, 2082), wherein the database is an LDAP Directory Server and communicates with other server/modules using LDAP over SSL" at page 6, [0119]. Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Dulin and Sinn's teachings to implement the certificate database using the

well-known LDAP directory server as suggested by Sinn, in order to take advantage of the legacy LDAP directory server to store digital certificates instead building a new database server for storing digital certificates, and therefore reduces the cost and the complexity of the system. Claims 1-6, 12-13, 16-22, 28-30 therefore remain rejected.

Conclusion

6. The prior art made of record, listed on form PTO-892, and not relied upon, if any, is considered pertinent to applicant's disclosure.

If a reference indicated as being mailed on PTO-FORM 892 has not been enclosed in this action, please contact Lisa Craney whose telephone number is **(571) 272-3574** for faster service.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Khanh B. Pham whose telephone number is (571) 272-4116. The examiner can normally be reached on Monday through Friday 7:30am to 4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John E Breene can be reached on (571) 272-4107. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Khanh B. Pham
Examiner
Art Unit 2167

December 20, 2004

A handwritten signature in black ink, appearing to read 'Khanh B. Pham', with a long horizontal flourish underneath.